



JFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:)
CALABRO' ET AL.)
Serial No. 10/736,237)
Confirmation No. 3158)
Filing Date: December 15, 2003)
For: METHOD OF PERFORMING A SIMON'S)
OR A SHOR'S QUANTUM ALGORITHM)
AND RELATIVE QUANTUM GATE)


TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

Sir:

Transmitted herewith is a certified copy of the
priority Italian Application No. VA2002A000069.

Respectfully submitted,


MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Telephone: 407/841-2330
Fax: 407/841-2343
Attorney for Applicant

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being
deposited with the United States Postal Service as first class
mail in an envelope addressed to: COMMISSIONER FOR PATENTS,
P.O. BOX 1450, ALEXANDRIA, VA 22313-1450, on this 21st day of
June, 2004.





Ministero delle Attività Produttive

Direzione Generale per lo Sviluppo Produttivo e la Competitività

Ufficio Italiano Brevetti e Marchi

Ufficio G2

Autenticazione di copia di documenti relativi alla domanda di brevetto per:

Invenzione Industriale

N. **VA2002 A 000069**



*Si dichiara che l'unita copia e noni documenti originali
depositati con la domanda di brevetto sopraspecificata, i cui dati
risultano dall'accluso processo verbale di deposito.*

Roma, il **20 NOV. 2003**

Per IL DIRIGENTE
Paola Giuliano
Dr.ssa Paola Giuliano

AL MINISTERO DELL'INDUSTRIA DEL COMMERCIO E DELL'ARTIGIANATO

MODULO A

UFFICIO ITALIANO BREVETTI E MARCHI - ROMA

DOMANDA DI BREVETTO PER INVENZIONE INDUSTRIALE, DEPOSITO RISERVE, ANTICIPATA ACCESSIBILITA' AL PUBBLICO



A. RICHIEDENTE (I)

1) Denominazione STMicroelectronics S.r.l. codice SR
 Residenza Agrate Brianza codice 00951900968
 2) Denominazione _____
 Residenza _____ codice _____

B. RAPPRESENTANTE DEL RICHIEDENTE PRESSO L'U.I.B.M.

cognome e nome Pellegrini Alberto ed altri cod. fiscale _____
 denominazione studio di appartenenza SOCIETA' ITALIANA BREVETTI S.p.A.
 via Piazza Repubblica n. 5 città VARESE cap 21100 (prov) VA

C. DOMICILIO ELETTIVO destinatario

via _____ n. _____ città _____ cap _____ (prov) _____
 classe proposta (sez/cl/sci) _____ gruppo/sottogruppo _____ / _____

D. TITOLO

METODO DI ESECUZIONE DI UN ALGORITMO QUANTISTICO DI SIMON O DI SHOR E RELATIVA GATE
QUANTISTICA

ANTICIPATA ACCESSIBILITA' AL PUBBLICO: SI ☐ NO ☒

SE ISTANZA: DATA ____/____/____

N. PROTOCOLLO

E. INVENTORI DESIGNATI

cognome nome

cognome nome

1) CALABRO' Antonino 3) _____
 2) PORTO Domenico 4) _____

F. PRIORITA'

nazione o organizzazione

tipo di priorità

numero di domanda

data di deposito

allegato
S/R

SCIOGLIMENTO RISERVE

Data

N° Protocollo

1) _____ / ____ / ____
 2) _____ / ____ / ____

G. CENTRO ABILITATO DI RACCOLTA COLTURE DI MICRORGANISMI, denominazione

H. ANNOTAZIONI SPECIALI

DOCUMENTAZIONE ALLEGATA

N. es.

Doc. 1) 2 PROV ☐ n. pag. 32 riassunto con disegno principale, descrizione e rivendicazione (obbligatorio 1 esemplare)
 Doc. 2) 2 PROV ☐ n. tav. 05 disegno (obbligatorio se citato in descrizione, 1 esemplare)
 Doc. 3) 1 RIS ☐ lettera d'incarico
 Doc. 4) 0 RIS ☐ designazione inventore
 Doc. 5) 0 RIS ☐ documenti di priorità con traduzione in italiano
 Doc. 6) 0 RIS ☐ autorizzazione o atto di cessione
 Doc. 7) 0 nominativo completo del richiedente

8) attestati di versamento, totale lire DUECENTONOVANTUNO/80 obbligatorio

COMPILATO IL 13/12/2002

FIRMA DEL (I) RICHIEDENTE (I)

Il Mandatario

Gaetano BARBARO
 N° Iscr. Albo 994 B

CONTINUA (SI/NO) NODEL PRESENTE ATTO SI RICHIEDE COPIA AUTENTICA (SI/NO) SI

CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA DI

VARESEcodice 12

VERBALE DI DEPOSITO

NUMERO DI DOMANDA

VA/2002/A/0069

Reg. A

L'anno due miladue il giorno TREDICI del mese di DICEMBRE
 Il (i) richiedente (i) sopraindicato (i) ha (hanno) presentato a me sottoscritto la presente domanda, corredata di n. 00 fogli aggiuntivi per la concessione del brevetto sopraportato.

ANNOTAZIONI VARIE DELL'UFFICIALE ROGANTE

NESSUNA

DANIELA GENNARO

IL DEPOSITANTE



LUISA DE ZORZI
 L'UFFICIALE ROGANTE

RIASSUNTO INVENZIONE CON DISEGNO PRINCIPALE

NUMERO DOMANDA

VA/2002/Al/0069

REG. A

DATA DI DEPOSITO

13 DIC. 2002

NUMERO BREVETTO

DATA DI RILASCIO

A. RICHIEDENTE (I)

Denominazione

STMicroelectronics S.r.l.

Residenza

Agrate Brianza (MI)

D. TITOLO

METODO DI ESECUZIONE DI UN ALGORITMO QUANTISTICO DI SIMON O DI SHOR E RELATIVA GATE QUANTISTICA

Classe proposta (sez./cl./scl/)

(gruppo/sottogruppo)

L. RIASSUNTO

Un metodo di esecuzione di un algoritmo quantistico di Simon o di Shor su una data funzione ($f(x)$) codificata con un certo numero n di qubits, comprende i seguenti passi di processo:

- eseguire un'operazione di sovrapposizione su un set di vettori d'ingresso, determinando un vettore di sovrapposizione,
- eseguire un'operazione di entanglement determinando un corrispondente vettore di entanglement,
- eseguire un'operazione di interferenza generando un corrispondente vettore di uscita.

Questo metodo consente di eseguire rapidamente l'operazione di sovrapposizione in quanto prevede di determinare il vettore di sovrapposizione individuando solo le componenti non nulle di esso calcolando, in funzione di detto numero di qubits n , il valore $1/2^{n/2}$ delle componenti non nulle del vettore di sovrapposizione, e calcolando indici di queste componenti come serie aritmetica di punto iniziale 1 e ragione pari a 2^n .

Questo metodo è implementato in una relativa gate quantistica hardware.

M. DISEGNO

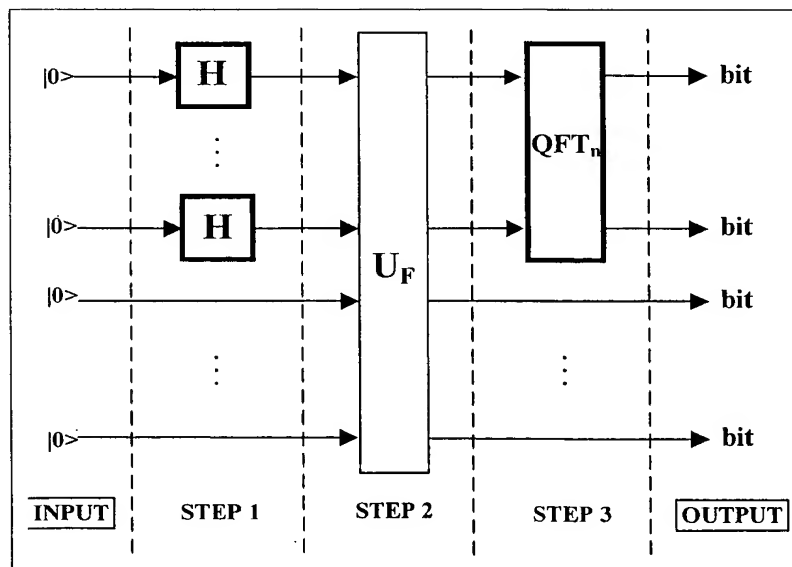


FIG. 6



13 DIC. 2002



Titolare: STMicroelectronics S.r.l.

**"METODO DI ESECUZIONE DI UN ALGORITMO QUANTISTICO
DI SIMON O DI SHOR E RELATIVA GATE QUANTISTICA"**

CAMPO DELL'INVENZIONE

La presente invenzione concerne in generale gli algoritmi quantistici e più precisamente un metodo e una relativa gate quantistica per eseguire algoritmi quantistici di Simon e di Shor in modo rapido, evitando di dover memorizzare matrici di dimensioni molto grandi.

BACKGROUND DELL'INVENZIONE

Gli algoritmi quantistici sono algoritmi casuali di ricerca basati su principi, leggi ed effetti quantistici della meccanica quantistica. Essi sono usati per controllare un processo o per processare dati in un database, e più in particolare per controllare un processo e/o includere operazioni intelligenti di ricerca dei minimi.

In operazioni di ricerca quantistica, ciascuna variabile è rappresentata da una sovrapposizione lineare finita di stati iniziali classici. Con una sequenza di passi elementari unitari di processo si manipola lo stato iniziale $|i\rangle$ (per l'ingresso) in modo che una misura dello stato finale del sistema fornisca l'uscita corretta. In generale, negli algoritmi quantistici sono usati tre operatori principali, la sovrapposizione lineare (*linear superposition*) tra stati coerenti, lo "aggrovigliamento" (*entanglement*) e l'interferenza (*interference*).

Per una migliore comprensione del campo di applicazione dell'invenzione, viene fatta una breve descrizione degli algoritmi quantistici.

INTRODUZIONE AGLI ALGORITMI QUANTISTICI

I problemi risolti dagli algoritmi quantistici possono essere formulati come segue:

Input	Una funzione $f: \{0,1\}^n \rightarrow \{0,1\}^m$
Problema	Trovare una certa proprietà di f

La struttura di un algoritmo quantistico è descritta ad alto livello nel diagramma di Figura 1. L'ingresso di un algoritmo quantistico è sempre una funzione f di una stringa binaria in una stringa binaria. Questa funzione è rappresentata come una tabella, definente per ciascuna stringa la sua immagine. La funzione f è prima codificata in un operatore matriciale unitario U_F che dipende dalle proprietà di f . In un certo senso, questo operatore calcola f quando le sue stringhe di ingresso e uscita sono codificate in settori di una base canonica di uno spazio complesso di Hilbert: U_F porta il codice vettoriale di ciascuna stringa nel codice vettoriale della sua immagine mediante f .

BOX 1: MATRICE UNITARIA U_F

Una matrice unitaria U_F sul campo complesso è *unitaria* se la sua matrice inversa coincide con la sua coniugata trasposta:

$$U_F^{-1} = U_F^\dagger$$

Una matrice unitaria è sempre reversibile e preserva la norma dei vettori.

Quando l'operatore matriciale U_F è stato generato, esso è implementato in una gate quantistica G , una matrice unitaria la cui struttura dipende dalla matrice U_F e dal problema che si vuole risolvere. La gate quantistica è il

cuore di un algoritmo quantistico. In ogni algoritmo quantistico, la gate quantistica agisce sulla base canonica iniziale di vettori (è possibile scegliere sempre lo stesso vettore) in modo da generare una combinazione lineare complessa (sovrapposizione) di vettori di base. Questa sovrapposizione contiene tutte le informazioni necessarie per rispondere al problema iniziale.

Dopo che questa sovrapposizione è stata effettuata, si esegue un'operazione di misura in modo da estrarre questa informazione. In meccanica quantistica, la misura è un'operazione non deterministica che produce come uscita solo uno dei vettori della base dell'operazione di sovrapposizione. La probabilità di ogni vettore della base di essere l'uscita della misura dipende dal suo coefficiente complesso (valore di probabilità) nella combinazione lineare complessa.

Ogni singola operazione della gate quantistica e la misura costituisce il blocco quantistico (quantum block). Il quantum block è ripetuto k volte in modo da produrre una collezione di k vettori di base. Dato che la misura è un'operazione non deterministica, questi vettori di base non saranno necessariamente identici e ciascuno di essi codificherà un pezzo dell'informazione necessaria a risolvere il problema.

L'ultima parte dell'algoritmo consiste nell'interpretazione dei vettori di base raccolti in modo da ricavare la risposta giusta al problema iniziale con una certa probabilità.

Encoder

Il comportamento del blocco codificatore (encoder) è descritto nello schema di dettaglio della Figura 2.

La funzione f è codificata nella matrice U_F in tre passi.



Passo 1

La tabella della funzione $f: \{0,1\}^n \rightarrow \{0,1\}^m$ è trasformata nella tabella della funzione iniettiva $F: \{0,1\}^{n+m} \rightarrow \{0,1\}^{n+m}$ in modo che:

$$F(x_0, \dots, x_{n-1}, y_0, \dots, y_{m-1}) = (x_0, \dots, x_{n-1}, f(x_0, \dots, x_{n-1}) \oplus (y_0, \dots, y_{m-1})) \quad (1)$$

BOX 2: OPERATORE XOR \oplus

L'operatore XOR tra due stringhe binarie p e q di lunghezza m è una stringa s di lunghezza m tale che l' i -esima cifra di s sia calcolata come la OR esclusiva tra l' i -esima cifra di p e q :

$$p = (p_0, \dots, p_{n-1})$$

$$q = (q_0, \dots, q_{n-1})$$

$$s = p \oplus q = ((p_0 + q_0) \bmod 2, \dots, (p_{n-1} + q_{n-1}) \bmod 2)$$

La necessità di avere a che fare con una funzione iniettiva viene dal requisito che U_F sia unitaria. Un operatore unitario è reversibile, per cui esso non può portare due diversi ingressi nella stessa uscita. Dal momento che U_F è la rappresentazione matriciale della funzione F , F deve essere iniettiva. Se si usasse direttamente la rappresentazione matriciale della funzione f , si otterrebbe una matrice non unitaria, dal momento che f potrebbe essere non iniettiva. Quindi, l'iniettività è soddisfatta incrementando il numero di bit e considerando la funzione F invece della funzione f . Comunque, la funzione f può sempre essere calcolata da F ponendo $(y_0, \dots, y_{m-1}) = (0, \dots, 0)$ nella stringa di ingresso e leggendo gli ultimi m valori della stringa di uscita.

Passo 2

La tabella della funzione F è trasformata nella tabella U_F secondo la seguente formula:

$$\forall s \in \{0,1\}^{n+m} : U_F[\tau(s)] = \tau[F(s)] \quad (2)$$



13 DIC. 2002

La mappa di codifica $\tau: \{0,1\}^{n+m} \rightarrow \mathbb{C}^{2^{n+m}}$ ($\mathbb{C}^{2^{n+m}}$ è lo spazio di Hilbert complesso di codominio) è tale che

$$\begin{aligned} \tau(0) &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle & \tau(1) &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \\ \tau(x_0, \dots, x_{n+m-1}) &= \tau(x_0) \otimes \dots \otimes \tau(x_{n+m-1}) = |x_0 \dots x_{n+m-1}\rangle \end{aligned} \quad (3)$$

BOX 3: PRODOTTO TENSORIALE VETTORIALE \otimes

Il prodotto tensoriale vettoriale tra due vettori di dimensioni h e k è un prodotto tensoriale vettoriale di dimensione $h \cdot k$, tale che:

$$|x\rangle \otimes |y\rangle = \begin{pmatrix} x_1 \\ \dots \\ x_h \end{pmatrix} \otimes \begin{pmatrix} y_1 \\ \dots \\ y_k \end{pmatrix} = \begin{pmatrix} x_1 y_1 \\ \dots \\ x_1 y_k \\ \dots \\ x_h y_1 \\ \dots \\ x_h y_k \end{pmatrix} \Rightarrow$$

Interpretazione fisica:

Se un componente di un vettore complesso è interpretato come la probabilità di un sistema di essere in un dato stato (indicato dal numero componente), il prodotto tensoriale tra due vettori descrive la probabilità congiunta di due sistemi di essere in uno stato congiunto.

Esempi: Prodotti Tensoriali Vettoriali

$$(0,0) \xrightarrow{\tau} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle$$

$$(0,1) \xrightarrow{\tau} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle$$

$$(1,0) \xrightarrow{\tau} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle$$

$$(1,1) \xrightarrow{\tau} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle$$

1 3 DIC. 2002



Il codice τ porta valori binari in vettori complessi di dimensione 2 appartenenti alla base canonica di \mathbb{C}^2 . Inoltre, usando il prodotto tensoriale, τ porta lo stato generale di una stringa binaria di dimensione n nel vettore di dimensione 2^n . Ciascuno stato è trasformato nel corrispondente vettore di base bidimensionale e lo stato della stringa è portato nel corrispondente vettore di base 2^n -dimensionale componendo tutti i vettori di bit attraverso il prodotto tensoriale. In questo senso il prodotto tensoriale è la controparte vettoriale della congiunzione di stato.

I vettori di base sono denotati usando la notazione *ket* $|i\rangle$. Questa notazione è presa dalla descrizione di Dirac della meccanica quantistica.

Passo 3

La tabella di U_F è trasformata nella matrice U_F usando la seguente regola di trasformazione:

$$[U_F]_{ij} = 1 \Leftrightarrow U_F |j\rangle = |i\rangle \quad (4)$$

Questa regola può essere facilmente compresa considerando i vettori $|i\rangle$ e $|j\rangle$ come vettori colonna. Dato che questi vettori appartengono alla base canonica, U_F definisce una mappa di permutazione delle righe della matrice identità. In generale, la riga $|j\rangle$ è trasformata nella riga $|i\rangle$.

Questa regola sarà illustrata in dettaglio nell'esempio di algoritmo quantistico: l'algoritmo di Shor.

Quantum Block

Il nocciolo del quantum block è la gate quantistica, che dipende dalle proprietà della matrice U_F . Lo schema in Figura 3 dà una descrizione più dettagliata del quantum block.

L'operatore matriciale U_F in Figura 3 è l'uscita del codificatore (encoder)

13 DIC. 2002

rappresentato in Figura 2. Qui, esso diventa l'ingresso per il blocco quantistico (quantum block).

Questo operatore matriciale è implementato in una gate più complessa: la gate quantistica G . La matrice unitaria G è applicata k volte ad un vettore di una base iniziale canonica $|i\rangle$ di dimensione 2^{n+m} . Ogni volta, si misura il risultato della sovrapposizione complessa $G|0..01..1\rangle$ di vettori di base, producendo un vettore di base $|x_i\rangle$ come risultato. Tutti i vettori di base misurati $\{|x_1\rangle, \dots, |x_k\rangle\}$ sono collezionati. Questa collezione è l'uscita del quantum block.

La "intelligenza" di questi algoritmi sta nella capacità di costruire una gate quantistica che sia capace di estrarre l'informazione necessaria per trovare la desiderata proprietà di f e di memorizzarla nella collezione di vettori di uscita.

La struttura della gate quantistica per ogni algoritmo quantistico sarà discussa in dettaglio, osservando che una descrizione generale è possibile.

Per poter rappresentare gate quantistiche verranno utilizzati alcuni diagrammi particolari chiamati circuiti quantistici (quantum circuits). Un esempio di un circuito quantistico è riportato in Figura 4. Ciascun rettangolo è associato ad una matrice $2^n \times 2^n$, in cui n è il numero di linee che entrano e lasciano il rettangolo. Per esempio, il rettangolo chiamato U_F è associato alla matrice U_F . Tipicamente

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (5)$$

I circuiti quantistici forniscono una descrizione ad alto livello della gate e, usando alcune regole di trasformazione, che sono illustrate nelle Figure da 5a

13 DIC. 2002

a 5f, è possibile comporre nella corrispondente matrice-gate.

BOX 4: PRODOTTO TENSORIALE MATRICIALE \otimes

Il prodotto tensoriale tra due matrici $X_{n \times m}$ e $Y_{h \times k}$ è una matrice $(n \cdot h) \times (m \cdot k)$ tale che:

$$X \otimes Y = \begin{bmatrix} x_{11}Y & \dots & x_{1m}Y \\ \dots & \dots & \dots \\ x_{n1}Y & \dots & x_{nm}Y \end{bmatrix} \quad \text{with} \quad X = \begin{bmatrix} x_{11} & \dots & x_{1m} \\ \dots & \dots & \dots \\ x_{n1} & \dots & x_{nm} \end{bmatrix}$$

Esempio: Prodotto Tensoriale Matriciale

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} = \begin{bmatrix} 1 \cdot \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} & 2 \cdot \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \\ 3 \cdot \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} & 4 \cdot \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 5 & 6 & 10 & 12 \\ 7 & 8 & 14 & 16 \\ 15 & 18 & 20 & 24 \\ 21 & 24 & 28 & 32 \end{bmatrix}$$

Sarà più chiaro come usare queste regole quando sarà trattato un esempio di algoritmo quantistico.

Decoder

Il blocco decodificatore (decoder) ha la funzione di interpretare i vettori di base collezionati dopo l'esecuzione iterata del blocco quantistico. Decodificare questi vettori significa tradurli di nuovo in una stringa binaria e interpretarli direttamente se essi già contengono la risposta al problema di partenza o utilizzarli, per esempio come vettori di coefficienti di qualche sistema di equazioni, in modo da ricavare la soluzione cercata. Questa parte non sarà trattata in dettaglio perché è una parte classica, facile e non interessante.

Per meglio descrivere ora un campo di applicazione dell'invenzione, verrà



trattato in dettaglio l'algoritmo quantistico di Shor.

L'ALGORITMO DI SHOR

Il problema di Shor può essere formulato nel seguente modo:

dato un numero intero N trovare un fattore p per N

Questo problema sembra essere alquanto diverso rispetto ai problemi risolti dagli algoritmi quantistici, ma esso può essere ridotto ad un problema equivalente che abbia la stessa forma di questi problemi. Questa riduzione è resa possibile da un risultato della teoria dei numeri che lega il periodo r di una speciale funzione periodica ai fattori di un intero N . Questa funzione è:

$$f_{N,a} : \mathbb{N} \rightarrow \mathbb{N} \text{ such that } f_{N,a}(x) = a^x \bmod N$$

in cui a è un numero casuale coprimo con N , cioè:

$$\gcd(a, N) = 1$$

in cui $\gcd(x, y)$ è il massimo comun divisore tra x e y .

Questa funzione è periodica (il periodo è al più N). Sia r tale periodo. Quindi:

$$f_{N,a}(0) = f_{N,a}(r) \quad a^r \equiv 1 \bmod N$$

Se il periodo è pari, questa equazione può essere riscritta come:

$$(a^{r/2})^2 \equiv 1 \bmod N \Leftrightarrow (a^{r/2})^2 - 1 \equiv 0 \bmod N \Leftrightarrow (a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \bmod N$$

questo significa che:

$$\exists h \in \mathbb{N} : (a^{r/2} - 1)(a^{r/2} + 1) = hN$$

quindi, a meno che $(a^{r/2} - 1) \equiv 0 \bmod N$ o $(a^{r/2} + 1) \equiv 0 \bmod N$, cioè $a^{r/2} \equiv \pm 1 \bmod N$, almeno una delle quantità $a^{r/2} + 1$ o $a^{r/2} - 1$ deve avere un fattore diverso da 1 in comune con N . Tale fattore può essere trovato calcolando:

$$\gcd(a^{r/2} - 1, N) \quad \gcd(a^{r/2} + 1, N)$$

Usando questa riduzione, la vera questione diventa: "qual è il periodo di f ?".

Dal momento che il periodo di questa funzione è minore di N , esso apparterrà

13 DIC. 2002

all'intervallo $[0, 1, \dots, N-1]$. Si codifica quindi un valore di ingresso come una stringa binaria. Sono necessari $n = \lceil \log N \rceil$ bit (eventualmente $\lceil \log N \rceil + 1$) per calcolare tutti gli N possibili valori di ingresso.

Quindi il problema di Shor è stato trasformato nel seguente problema quantistico standard:

Input	$f: \{0,1\}^n \rightarrow \{0,1\}^n$ con periodo r
Problema	Calcolare r

ENCODER

Per meglio illustrare l'algoritmo quantistico di Shor si farà dapprima riferimento ad un esempio introduttivo. Poi si generalizzano le conclusioni.

A. Esempio Introduttivo

Si consideri il caso:

$$N = 4 \Rightarrow n = 2; \quad a = 3$$

La tabella che descrive f è:

(x_0, x_1)	$f(x_0, x_1)$
00	01
01	11
10	01
11	11

Tab. 1

Il periodo di questa funzione è $r = 2$.

Passo 1

La funzione f è codificata nella funzione iniettiva F costruita usando la formula 2. La tabella di f è quindi:

$(x_0, \dots, x_{n-1}, y_0, \dots, y_{n-1})$	$F(x_0, \dots, x_{n-1}, y_0, \dots, y_{n-1})$
0000	0001
0100	0111
1000	1001
1100	1111
0001	0000
0101	0110

13 DIC. 2002



1001	1000
1101	1110
0010	0011
0110	0101
1010	1011
1110	1101
0011	0010
0111	0100
1011	1010
1111	1100

Tab. 2

Passo 2

Si codifica ora la funzione F nella tabella dell'operatore U_F :

$ x_0 \dots x_{n-1} y_0 \dots y_{n-1}\rangle$	$U_F x_0 \dots x_{n-1} y_0 \dots y_{n-1}\rangle$
$ 0000\rangle$	$ 0001\rangle$
$ 0100\rangle$	$ 0111\rangle$
$ 1000\rangle$	$ 1001\rangle$
$ 1100\rangle$	$ 1111\rangle$
$ 0001\rangle$	$ 0000\rangle$
$ 0101\rangle$	$ 0110\rangle$
$ 1001\rangle$	$ 1000\rangle$
$ 1101\rangle$	$ 1110\rangle$
$ 0010\rangle$	$ 0011\rangle$
$ 0110\rangle$	$ 0101\rangle$
$ 1010\rangle$	$ 1011\rangle$
$ 1110\rangle$	$ 1101\rangle$
$ 0011\rangle$	$ 0010\rangle$
$ 0111\rangle$	$ 0100\rangle$
$ 1011\rangle$	$ 1010\rangle$
$ 1111\rangle$	$ 1100\rangle$

Tab. 3

Passo 3

La matrice corrispondente a U_F è ottenuta utilizzando la seguente regola:

$$[U_F]_{ij} = 1 \Leftrightarrow U_F|j\rangle = |i\rangle$$

o più semplicemente osservando che i primi due vettori nel prodotto tensoriale di ingresso non sono cambiati, mentre l'operatore che agisce sugli ultimi due vettori è scelto nell'insieme $\{I \otimes I, I \otimes C, C \otimes I, C \otimes C\}$, in cui I è la matrice identità e C è la matrice complemento, che dipende dai valori dei

primi due vettori:

U_F	$ 00\rangle$	$ 01\rangle$	$ 10\rangle$	$ 11\rangle$
$ 00\rangle$	$I \otimes C$	0	0	0
$ 01\rangle$	0	$C \otimes C$	0	0
$ 10\rangle$	0	0	$I \otimes C$	0
$ 11\rangle$	0	0	0	$C \otimes C$

Tab. 4

Questa matrice conserva i primi due vettori e:

- conserva il terzo e inverte il quarto quando il secondo vettore è $|0\rangle$;
- inverte il terzo e il quarto quando il secondo vettore è $|1\rangle$.

Si osservi che il blocco matriciale di posto (i, i) è identico al blocco matriciale di posto $((i+r) \bmod N, (i+r) \bmod N)$ in cui i è l'indice binario del vettore che indica la riga e la colonna della matrice individuanti la cella.

B. Caso generale con $n = 2$

In generale, se $n = 2$, prendendo un diverso valore per a e quindi un diverso periodo r , l'operatore trasforma ancora i primi n vettori in sé stessi, ma i blocchi matriciali sulla diagonale principale cambiano.

La matrice U_F ha la seguente forma:

U_F	$ 00\rangle$	$ 01\rangle$	$ 10\rangle$	$ 11\rangle$
$ 00\rangle$	M_{00}	0	0	0
$ 01\rangle$	0	M_{01}	0	0
$ 10\rangle$	0	0	M_{10}	0
$ 11\rangle$	0	0	0	M_{11}

Tab. 5

in cui $M_i \in \{I \otimes I, I \otimes C, C \otimes I, C \otimes C\}$ e $M_i = M_j \Leftrightarrow ((j=i) \text{ OR } (j=(i+r) \bmod N))$.

C. Caso Generale

Ragionando nello stesso modo, è possibile dedurre la seguente forma generale della matrice U_F quando $n > 0$:

U_F	$ 0..0\rangle$	$ 0..1\rangle$...	$ 1..1\rangle$
$ 0..0\rangle$	$M_{0..0}$	0	...	0
$ 0..1\rangle$	0	$M_{0..1}$...	0
...



$ 1..1\rangle$	0	0	0	$M_{1..1}$
----------------	---	---	---	------------

Tab. 6

in cui $M_i = P_1 \otimes \dots \otimes P_n$, $P_k \in \{I, C\}$, $k=1, \dots, n$ e $M_i = M_j \Leftrightarrow ((j=i) \text{ OR } (j=(i+r) \bmod N))$.

Le etichette delle colonne sono vettori di base di dimensione n .

QUANTUM BLOCK

La gate quantistica di Shor può essere descritta con il circuito quantistico riportato in Figura 6.

La gate quantistica dell'algoritmo di Shor mostrata in Figura 7 è simile alla gate quantistica dell'algoritmo quantistico di Simon mostrata in Figura 8, tranne che per l'operatore interferenza. Nell'algoritmo di Simon si applica l'operatore H ai primi n vettori in uscita da U_F . Questo operatore dell'algoritmo di Simon causa l'annullamento di alcune celle della prima colonna della gate finale e questo produce una particolare sovrapposizione dei vettori di base come uscita. Misurando questa sovrapposizione è possibile risolvere il problema di Simon.

Nell'algoritmo di Shor l'operatore interferenza (cioè l'operatore finale) non è H , dal momento che la diagonale principale di U_F è diversa ed è necessario un diverso operatore interferenza in modo da estrarre informazione. Questo operatore è rappresentato dalla matrice QFT_n , chiamata Trasformata Quantistica di Fourier di ordine n . Questo operatore è non-classico dal momento che esso trasforma un vettore di base in una combinazione lineare complessa di vettori di base. In generale, un vettore di base $|i\rangle$ è trasformato nella combinazione lineare $\alpha_1 y_1 + \dots + \alpha_n y_n$ in cui α_i and α_{i+1} hanno lo stesso modulo $1/2^{n/2}$ ma sono sfasati di $i \cdot (2\pi/2^n)$ a partire da $\alpha_1 = 1/2^{n/2}$. Questo operatore è definito dalla seguente tabella

QFT_n	$\phi=0$	$\phi=2\pi/2^n$...	$\phi=(2^n-1)2\pi/2^n$
$ 0..0\rangle$	$ 0..0\rangle$	$ 0..1\rangle$...	$ 1..1\rangle$
$ 0..0\rangle$	$1/2^{n/2}$	$1/2^{n/2}$...	$1/2^{n/2}$
$ 0..1\rangle$	$1/2^{n/2}$	$1/2^{n/2} e^{J2\pi/2^n}$...	$1/2^{n/2} e^{J(2^n-1)2\pi/2^n}$
...
$ 1..1\rangle$	$1/2^{n/2}$	$1/2^{n/2} e^{J(2^n-1)2\pi/2^n}$...	$1/2^{n/2} e^{J(2^n-1)^2 2\pi/2^n}$

Tab. 7

in cui J è l'unità immaginaria. Applicando le regole di trasformazione delle Figure da 5a a 5f al circuito di Figura 6, si ottiene la gate quantistica di Figura 7.

Verranno discusse la forma di queste gate in alcuni casi speciali e poi le osservazioni fatte verranno generalizzate.

A. Esempio Introduttivo

Nel caso $n = 2$, la gate quantistica ha la seguente forma:

$$G=(QFT_2 \otimes^2 I) \cdot U_F \cdot (^2 H \otimes^2 I)$$

si calcola ora questa gate per l'esempio introduttivo:

$^2 H \otimes^2 I$	$ 00\rangle$	$ 01\rangle$	$ 10\rangle$	$ 11\rangle$
$ 00\rangle$	$^2 I/2$	$^2 I/2$	$^2 I/2$	$^2 I/2$
$ 01\rangle$	$^2 I/2$	$^{-2} I/2$	$^2 I/2$	$^{-2} I/2$
$ 10\rangle$	$^2 I/2$	$^2 I/2$	$^{-2} I/2$	$^{-2} I/2$
$ 11\rangle$	$^2 I/2$	$^{-2} I/2$	$^{-2} I/2$	$^2 I/2$

Tab. 8

La matrice U_F è già stata rappresentata nella Tabella 4.

$U_F(^2 H \otimes^2 I)$	$ 00\rangle$	$ 01\rangle$	$ 10\rangle$	$ 11\rangle$
$ 00\rangle$	$I \otimes C/2$	$I \otimes C/2$	$I \otimes C/2$	$I \otimes C/2$
$ 01\rangle$	$C \otimes C/2$	$-C \otimes C/2$	$C \otimes C/2$	$-C \otimes C/2$
$ 10\rangle$	$I \otimes C/2$	$I \otimes C/2$	$-I \otimes C/2$	$-I \otimes C/2$
$ 11\rangle$	$C \otimes C/2$	$-C \otimes C/2$	$-C \otimes C/2$	$C \otimes C/2$

Tab. 9

Se $n = 2$, QFT_2 è la seguente:

QFT_2	$\phi=0$	$\phi=\pi/2$	$\phi=\pi$	$\phi=3\pi/2$
$ 00\rangle$	$ 00\rangle$	$ 01\rangle$	$ 10\rangle$	$ 11\rangle$
$ 00\rangle$	$1/2$	$1/2$	$1/2$	$1/2$
$ 01\rangle$	$1/2$	$J/2$	$-1/2$	$-J/2$
$ 10\rangle$	$1/2$	$-1/2$	$1/2$	$-1/2$

13 DIC. 2002

$ 11\rangle$	$1/2$	$-J/2$	$-1/2$	$J/2$
--------------	-------	--------	--------	-------

Tab. 10

$QFT_2 \otimes^2 I$	$ 00\rangle$	$ 01\rangle$	$ 10\rangle$	$ 11\rangle$
$ 00\rangle$	$^2I/2$	$^2I/2$	$^2I/2$	$^2I/2$
$ 01\rangle$	$^2I/2$	$J^2I/2$	$^{-2}I/2$	$-J^2I/2$
$ 10\rangle$	$^2I/2$	$^{-2}I/2$	$^2I/2$	$^{-2}I/2$
$ 11\rangle$	$^2I/2$	$-J^2I/2$	$^{-2}I/2$	$J^2I/2$

Tab. 11

Si calcola quindi la tabella della gate quantistica G :

G	$ 00\rangle$	$ 01\rangle$	$ 10\rangle$	$ 11\rangle$
$ 00\rangle$	$(I \otimes C + C \otimes C)/2$	$(I \otimes C - C \otimes C)/2$	0	0
$ 01\rangle$	0	0	$(I \otimes C + J C \otimes C)/2$	$(I \otimes C - J C \otimes C)/2$
$ 10\rangle$	$(I \otimes C - C \otimes C)/2$	$(I \otimes C + C \otimes C)/2$	0	0
$ 11\rangle$	0	0	$(I \otimes C - J C \otimes C)/2$	$(I \otimes C + J C \otimes C)/2$

Tab. 12

Applicando l'operatore G al vettore $|0000\rangle$ si ha:

$$G|0000\rangle = |00\rangle \frac{1}{2} (I \otimes C + C \otimes C) |00\rangle + |10\rangle \frac{1}{2} (I \otimes C - C \otimes C) |00\rangle$$

Se si effettua una misura di questo vettore e si trasformano i primi due vettori di dimensione 2 nelle loro etichette binarie, i possibili risultati sono:

00 con probabilità 0.5

10 con probabilità 0.5

La distanza tra questi valori è $d = [|10-00|]_{10} = [10]_{10} = 2$, in cui $[s]_{10}$ è la rappresentazione decimale della stringa binaria s . Si osservi che $N/r = 4/2 = 2$.

Quindi $d = N/r$. Se r è incognito, allora esso può essere calcolato come:

$$r = N/d$$

B. Caso generale con $n = 2, r = 2$

Si è visto che quando $n = 2$, la gate quantistica ha la seguente forma:

$$G = (QFT_2 \otimes^2 I) \cdot U_F \cdot (^2H \otimes^2 I)$$

usando le matrici calcolate nell'esempio introduttivo e ricordando che U_F è

13 DIC. 2002



data dalla Tabella 5.

$U_F(^2H \otimes ^2I)$	$ 00\rangle$	$ 01\rangle$	$ 10\rangle$	$ 11\rangle$
$ 00\rangle$	$M_{00}/2$	$M_{00}/2$	$M_{00}/2$	$M_{00}/2$
$ 01\rangle$	$M_{01}/2$	$-M_{01}/2$	$M_{01}/2$	$-M_{01}/2$
$ 10\rangle$	$M_{10}/2$	$M_{10}/2$	$-M_{10}/2$	$-M_{10}/2$
$ 11\rangle$	$M_{11}/2$	$-M_{11}/2$	$-M_{11}/2$	$M_{11}/2$

Tab. 13

Ricordando l'espressione dell'operatore interferenza $QFT_2 \otimes ^2I$ riportato in Tabella 11, si trova la seguente forma generalizzata di G :

G	$ 00\rangle$	$ 01\rangle$	$ 10\rangle$	$ 11\rangle$
$ 00\rangle$	$(M_{00}+M_{01}+M_{10}+M_{11})/4$	$(M_{00}-M_{01}+M_{10}-M_{11})/4$	$(M_{00}+M_{01}-M_{10}-M_{11})/4$	$(M_{00}-M_{01}-M_{10}+M_{11})/4$
$ 01\rangle$	$(M_{00}+JM_{01}-M_{10}-JM_{11})/4$	$(M_{00}-JM_{01}-M_{10}+JM_{11})/4$	$(M_{00}+JM_{01}+M_{10}+JM_{11})/4$	$(M_{00}-JM_{01}+M_{10}-JM_{11})/4$
$ 10\rangle$	$(M_{00}-M_{01}+M_{10}-M_{11})/4$	$(M_{00}+M_{01}+M_{10}+M_{11})/4$	$(M_{00}-M_{01}-M_{10}+M_{11})/4$	$(M_{00}+M_{01}-M_{10}-M_{11})/4$
$ 11\rangle$	$(M_{00}-JM_{01}-M_{10}+JM_{11})/4$	$(M_{00}+JM_{01}-M_{10}-JM_{11})/4$	$(M_{00}-JM_{01}+M_{10}-JM_{11})/4$	$(M_{00}+JM_{01}+M_{10}+JM_{11})/4$

Tab. 14

Se $r = 2$, come nell'esempio introduttivo, allora $M_{00}=M_{10} \neq M_{01}=M_{11}$. Questo significa che:

G	$ 00\rangle$	$ 01\rangle$	$ 10\rangle$	$ 11\rangle$
$ 00\rangle$	$(M_{00}+M_{01})/2$	$(M_{00}-M_{01})/2$	0	0
$ 01\rangle$	0	0	$(M_{00}+JM_{01})/2$	$(M_{00}-JM_{01})/2$
$ 10\rangle$	$(M_{00}-M_{01})/2$	$(M_{00}+M_{01})/2$	0	0
$ 11\rangle$	0	0	$(M_{00}-JM_{01})/2$	$(M_{00}+JM_{01})/2$

Tab. 15

Applicando l'operatore G al vettore $|0000\rangle$:

$$G|0000\rangle = |00\rangle \frac{1}{2}(M_{00} + M_{01})|00\rangle + |10\rangle \frac{1}{2}(M_{00} - M_{01})|00\rangle$$

Se si effettua una misura di questo vettore e si trasformano i primi due vettori di dimensione 2 nelle loro etichette binarie, allora i risultati possibili sono:

00 con probabilità 0.5

10 con probabilità 0.5

Questi sono gli stessi risultati ottenuti per l'esempio introduttivo, per cui possono essere ripetute le stesse considerazioni.



13 DIC. 2002

C. Caso generale

Si è visto che nel caso generale, l'operatore U_F è definito dalla Tabella 6. Si

vuole ora calcolare la gate quantistica G nella situazione generale:

${}^nH \otimes {}^nI$	$ 0..0\rangle$...	$ j\rangle$...	$ 1..1\rangle$
$ 0..0\rangle$	${}^nI/2^{n/2}$...	${}^nI/2^{n/2}$...	${}^nI/2^{n/2}$
$ 0..1\rangle$	${}^nI/2^{n/2}$...	$(-1)^{(0..1) \cdot j} ({}^nI/2^{n/2})$...	$-{}^nI/2^{n/2}$
...
$ i\rangle$	${}^nI/2^{n/2}$...	$(-1)^{ij} ({}^nI/2^{n/2})$...	$(-1)^{i \cdot (1..1)} ({}^nI/2^{n/2})$
...
$ 1..1\rangle$	${}^nI/2^{n/2}$...	$(-1)^{(1..1)j} ({}^nI/2^{n/2})$...	$(-1)^{(1..1) \cdot (1..1)} ({}^nI/2^{n/2})$

Tab. 16

$U_F \cdot ({}^nH \otimes {}^nI)$	$ 0..0\rangle$...	$ j\rangle$...	$ 1..1\rangle$
$ 0..0\rangle$	$M_{0..0}/2^{n/2}$...	$M_{0..0}/2^{n/2}$...	$M_{0..0}/2^{n/2}$
...
$ i\rangle$	$M_i/2^{n/2}$...	$(-1)^{ij} M_i/2^{n/2}$...	$(-1)^{i \cdot (1..1)} M_i/2^{n/2}$
...
$ 1..1\rangle$	$M_{1..1}/2^{n/2}$...	$(-1)^{(1..1)j} M_{1..1}/2^{n/2}$...	$(-1)^{(1..1) \cdot (1..1)} M_{1..1}/2^{n/2}$

Tab. 17

Dato che:

$$[QFT]_{i,j} = \frac{1}{2^{n/2}} e^{j[i]_{10} \frac{[j]_{10} \cdot 2\pi}{2^n}}$$

in cui $[i]_{10}$ and $[j]_{10}$ sono rappresentazioni decimali delle stringhe binarie i e j ,

si ha:

$QFT_n \otimes {}^nI$	$ 0..0\rangle$...	$ j\rangle$...	$ 1..1\rangle$
$ 0..0\rangle$	${}^nI/2^{n/2}$...	${}^nI/2^{n/2}$...	${}^nI/2^{n/2}$
...
$ i\rangle$	${}^nI/2^{n/2}$...	${}^nI/2^{n/2} e^{j[i]_{10} \cdot [j]_{10} 2\pi/2^n}$...	${}^nI/2^{n/2} e^{j[i]_{10} \cdot (2^n - 1) 2\pi/2^n}$
...
$ 1..1\rangle$	${}^nI/2^{n/2}$...	${}^nI/2^{n/2} e^{j(2^n - 1) \cdot [j]_{10} 2\pi/2^n}$...	${}^nI/2^{n/2} e^{j(2^n - 1)^2 2\pi/2^n}$

Tab. 18

La gate quantistica G ha la seguente forma:

G	$ 0..0\rangle$...
$ 0..0\rangle$	$1/2^n \sum_{k \in \{0,1\}^n} e^{j\pi \cdot 0 \cdot [k]_{10} / 2^{n-1}} M_k$...
...
$ i\rangle$	$1/2^n \sum_{k \in \{0,1\}^n} e^{j\pi \cdot [i]_{10} \cdot [k]_{10} / 2^{n-1}} M_k$...

$$\left| \begin{array}{ccc} \dots & & \dots \\ |1\dots 1\rangle & 1/2^n \sum_{k \in \{0,1\}^n} e^{j\pi \cdot (2^n - 1) \cdot [k]_{10} / 2^{n-1}} M_k & \dots \end{array} \right|$$

Tab. 19

Si consideri il generico termine

$$1/2^n \sum_{k \in \{0,1\}^n} e^{j\pi \cdot [i]_{10} \cdot [k]_{10} / 2^{n-1}} M_k$$

Dato che $M_i = P_1 \otimes \dots \otimes P_n$, $P_k \in \{I, C\}$, $k=1, \dots, n$ e $M_i = M_j \Leftrightarrow$

(($j=i$) OR ($j=(i+r) \bmod N$)), questo termine può essere scritto come

$$1/2^n \sum_{h \in R} [e^{j\pi \cdot [i]_{10} \cdot [h]_{10} / 2^{n-1}} + e^{j\pi \cdot [i]_{10} \cdot ([h]_{10} + 1)r / 2^{n-1}} + \dots + e^{j\pi \cdot [i]_{10} \cdot ([h]_{10} + (l_h - 1)r) / 2^{n-1}}] M_h$$

oppure

$$1/2^n \sum_{h \in R} (-1)^{[h]_{10} [i]_{10} / 2^{n-1}} [(-1)^{0r [i]_{10} / 2^{n-1}} + (-1)^{1r [i]_{10} / 2^{n-1}} + \dots + (-1)^{(l_h - 1)r [i]_{10} / 2^{n-1}}] M_h$$

in cui $R = \{0\dots 0, 0\dots 1, \dots, [r-1]_2\}$.

Si supponga che N sia multiplo di r , allora $l_h = 2^n / r = l$ per ogni h . Quindi, il

termine precedente può essere trasformato in:

$$1/2^n \sum_{h \in R} (-1)^{[h]_{10} [i]_{10} / 2^{n-1}} [(-1)^{2 \cdot 0 \cdot [i]_{10} / l} + (-1)^{2 \cdot 1 \cdot [i]_{10} / l} + \dots + (-1)^{2 \cdot (l-1) \cdot [i]_{10} / l}] M_h$$

ed infine:

$$1/2^n \sum_{h \in R} (-1)^{[h]_{10} [i]_{10} / 2^{n-1}} [e^{j \cdot 0 \cdot (2\pi [i]_{10} / l)} + e^{j \cdot 1 \cdot (2\pi [i]_{10} / l)} + \dots + e^{j \cdot (l-1) \cdot (2\pi [i]_{10} / l)}] M_h$$

Il termine:

$$e^{j \cdot 0 \cdot (2\pi [i]_{10} / l)} + e^{j \cdot 1 \cdot (2\pi [i]_{10} / l)} + \dots + e^{j \cdot (l-1) \cdot (2\pi [i]_{10} / l)}$$

è la somma delle l radici di ordine l dell'unità, a meno che i non sia multiplo di l . La somma delle radici dell'unità di dato ordine è sempre nulla. Di conseguenza, nella prima colonna di G solo quelle celle la cui etichetta di riga è $|i\rangle$ con i multiplo di l sono diverse da 0. Questo significa che applicando l'operatore G al vettore $|0\dots 0\rangle$, misurando il risultato e trasformando i primi n vettori di base di dimensione 1 del risultante prodotto tensoriale nei loro valori binari, si ottengono solo stringhe i tali che $i = m \cdot l$ per qualche intero m questo significa $i \equiv 0 \bmod l$.

13 DIC. 2002

DECODER

Il quantum block, così come accade per l'algoritmo di Simon, è ripetuto diverse volte in modo da costruire una collezione di vettori $|i\rangle$ tali che $i \equiv 0 \pmod{L}$. Mettendo queste equazioni a sistema e risolvendole, si ottiene il valore di L . Dal momento che $L=2^n/r$, si calcola $r=2^n/L$.

Il numero di vettori necessari per calcolare r dipende dalla tecnica usata per risolvere il sistema di equazioni. In generale, è necessario ripetere il quantum block un numero di volte che cresce con legge polinomiale con n .

Se 2^n non è multiplo di r , allora $l_h = \lceil 2^n/r \rceil$ per qualche h , $l_h = \lceil 2^n/r \rceil + 1$ per qualche altro h . Il termine

$$e^{j \cdot 0 (2\pi [i]_{10}/l_h)} + e^{j \cdot 1 (2\pi [i]_{10}/l_h)} + \dots + e^{j \cdot (l_h - 1) (2\pi [i]_{10}/l_h)}$$

non è esattamente 0 quando i non è multiplo di l_h , ma esso è prossimo a 0. Quindi, tutte le possibili stringhe possono essere trovate come risultato di un'operazione di misura, ma le stringhe i che non rappresentano un multiplo di $2^n/r$ difficilmente saranno osservate. Per diminuire questa probabilità (ed incrementare la probabilità dei multipli di $2^n/r$) si usano $2n$ bit di ingresso per codificare f . Questo significa che più radici dell'unità sono coinvolte e quindi è raggiunta una migliore approssimazione.

Seguendo gli approcci classici, appare evidente che il numero di bit quantistici (qubit) di un algoritmo quantistico può essere un parametro critico che limita notevolmente la velocità di calcolo. Infatti, riferendosi allo schema di Figura 6, si può notare che l'aggiunta di un solo qubit raddoppia la dimensione delle matrici rispetto alla precedente configurazione e il numero di elementi (e di prodotti) cresce esponenzialmente. Questo fatto limita la possibilità di utilizzare l'algoritmo di Shor e l'algoritmo di Simon in casi

13 DIC. 2002



pratici di effettivo interesse in cui il numero di qubit n può essere relativamente elevato.

SCOPO E SOMMARIO DELL'INVENZIONE

È stato trovato ed è l'oggetto della presente invenzione un metodo per eseguire rapidamente algoritmi quantistici di Simon o di Shor.

Diversamente dai metodi noti, secondo il metodo dell'invenzione non viene generato l'operatore matriciale di sovrapposizione, e non vengono effettuati i prodotti riga-colonna, perché si calcolano solo gli indici delle componenti non nulle dei vettori generati dall'operazione di sovrapposizione. In questo modo si devono calcolare e memorizzare solo vettori di 2^n di componenti, con notevole risparmio di tempo e di memoria.

Più precisamente un oggetto dell'invenzione è un metodo di esecuzione di un algoritmo quantistico di Simon o di Shor su una data funzione ($f(x)$) codificata con un certo numero n di qubits, comprendente

- eseguire un'operazione di sovrapposizione su un set di vettori d'ingresso, determinando un vettore di sovrapposizione,
- eseguire un'operazione di entanglement determinando un corrispondente vettore di entanglement,
- eseguire un'operazione di interferenza generando un corrispondente vettore di uscita.

Il metodo dell'invenzione consente di eseguire rapidamente l'operazione di sovrapposizione in quanto prevede di determinare il vettore di sovrapposizione individuando solo le componenti non nulle di esso calcolando, in funzione di detto numero di qubits n , il valore $1/2^{n/2}$ delle componenti non nulle del vettore di sovrapposizione, e calcolando indici di



queste componenti come serie aritmetica di punto iniziale 1 e ragione pari a 2^n .

Secondo una forma di realizzazione preferita, vengono eseguite operazioni analoghe per semplificare l'operazione di entanglement.

Il metodo dell'invenzione è implementato in una relativa gate quantistica avente

- un sottosistema di sovrapposizione eseguente un'operazione di sovrapposizione (superposition) secondo un algoritmo quantistico di Simon o di Shor su un set di vettori d'ingresso, determinante un vettore di sovrapposizione;
- un sottosistema di entanglement elaborante componenti del vettore di sovrapposizione, determinante un corrispondente vettore di entanglement; e
- un sottosistema di interferenza elaborante componenti del vettore di entanglement, generando un corrispondente vettore di uscita.

La particolarità della gate quantistica dell'invenzione consiste nel fatto che il sottosistema di sovrapposizione comprende

- un circuito generante una prima stringa di bit rappresentativa del valore $1/2^{n/2}$ delle componenti non nulle del vettore di sovrapposizione e altre 2^n stringhe di bit ciascuna rappresentativa di un rispettivo indice delle 2^n componenti non nulle del vettore di sovrapposizione, e
- un buffer di memoria memorizzante le stringhe rappresentanti il valore $1/2^{n/2}$ e questi indici.

L'invenzione è più precisamente descritta nelle annesse rivendicazioni.

13 DIC. 2002

BREVE DESCRIZIONE DEI DISEGNI

I diversi aspetti e vantaggi dell'invenzione risulteranno ancor più evidenti attraverso una descrizione dettagliata facendo riferimento ai disegni allegati, in cui:

la **Figura 1** è uno schema a blocchi degli algoritmi quantistici;

la **Figura 2** è uno schema a blocchi di un Encoder;

la **Figura 3** è una struttura generale del Quantum Block di Figura 1;

la **Figura 4** è un circuito per una gate quantistica di Deutsch-Jozsa's;

la **Figura 5a** mostra un esempio di trasformazione prodotto tensoriale;

la **Figura 5b** mostra un esempio di trasformazione prodotto semplice (dot product);

la **Figura 5c** mostra la trasformazione identità;

la **Figura 5d** mostra un esempio di regola di propagazione;

la **Figura 5e** mostra un esempio di regola di iterazione;

la **Figura 5f** illustra la regola tensoriale ingresso/uscita;

la **Figura 6** illustra il circuito quantistico dell'algoritmo di Shor;

la **Figura 7** illustra la gate quantistica dell'algoritmo di Shor;

la **Figura 8** illustra la gate quantistica dell'algoritmo di Simon.

DESCRIZIONE DI UNA FORMA DI REALIZZAZIONE DELL'INVENZIONE

Sia per l'algoritmo di Shor che per l'algoritmo di Simon, il blocco di sovrapposizione è dato da $H \otimes I$. Questo significa che i primi n qubit del vettore d'ingresso devono essere moltiplicati per H e i secondi n qubit devono essere moltiplicati per I .

Per mostrare meglio come si può semplificare l'operazione di sovrapposizione, si considera prima il seguente esempio con $n=3$. I primi 3

13 DIC. 2002

qubit del vettore P generato dall'operatore di sovrapposizione saranno dati da:

$$H|0\rangle \otimes H|0\rangle \otimes H|0\rangle$$

Trascurando il fattore costante $1/2^{3/2}$ ($n=3$), questo prodotto tensoriale sarà uguale a:

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 1 \end{bmatrix} = [1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1]^T$$

In generale, il vettore P generato con l'operazione di sovrapposizione sarà

$$P = [p_1 \ p_2 \ \dots \ p_{2^n}]$$

in cui $p_i = 1/2^{n/2}$.

Nell'esempio per $n=3$, il vettore P è dato da

$$P = \frac{1}{2^{3/2}} \cdot [1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1]^T \otimes [1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0]^T$$

Nel caso generale (n qualsiasi) le componenti p_i del vettore P ottenuto con l'operazione di sovrapposizione secondo l'algoritmo di Shor o di Simon saranno date da:

$$p_i = \begin{cases} \frac{1}{2^{n/2}} & \text{se } i = 1 + 2^n(j-1) \\ 0 & \text{altrove} \end{cases} \quad (6)$$

con $j = 1 \dots 2^n$, $i = 1 \dots 2^{2n}$.

Come si può chiaramente vedere, le componenti del vettore di sovrapposizione possono assumere solo due valori, di cui solo 2^n sono diversi da zero e devono essere memorizzati. Il grande vantaggio rispetto ai metodi noti consiste nel fatto che non è più necessario memorizzare l'operatore di sovrapposizione ${}^n H \otimes {}^n I$, che ha dimensione $2^{2n} \times 2^{2n}$, ed eseguire i prodotti riga-colonna, ma si possono memorizzare solo le posizioni delle 2^n componenti non nulle del vettore di sovrapposizione. Il valore non nullo di tali componenti è $1/2^{n/2}$ ed è immediatamente calcolabile conoscendo il



numero n di qubits.

Secondo il metodo dell'invenzione, il vettore di sovrapposizione P non è calcolato effettuando 2^{2n} prodotti riga-colonna, come nei metodi noti, ma è determinato semplicemente calcolando le posizioni delle 2^n componenti non nulle, essendo il loro valore $1/2^{n/2}$.

Questi indici possono essere facilmente calcolati, ad esempio in forma di stringhe di bit, con un CPLD (Complex Programmable Logic Device), semplicemente fornendo il numero n di qubit.

Un altro scopo della presente invenzione è quello di semplificare l'operazione di entanglement.

È stato notato che in tutti gli algoritmi quantistici, la matrice di entanglement U_F è una matrice diagonale a blocchi la cui struttura è intimamente legata alla rappresentazione binaria della funzione f . I blocchi matriciali diagonali possono essere la matrice identità I o complemento C o le matrici ottenute come prodotti tensoriali di esse.

Ad esempio per l'algoritmo di Shor, con $n=2$, i blocchi matriciali della matrice U_F sono scelti nell'insieme composto da

$$I \otimes I, I \otimes C, C \otimes I, C \otimes C$$

ciascuno di dimensione $2^2 \times 2^2$. Questi blocchi matriciali possono immediatamente essere ricavati a partire dalla Tabella 1 notando che, se ad un certo vettore (x_0, x_1) corrisponde il valore 00, allora il blocco matriciale sulla diagonale di U_F in corrispondenza della riga $|x_0, x_1\rangle$ è pari a $I \otimes I$. Similmente, se $f(x_0, x_1)$ è uguale a 01, o 10 o 11, il blocco matriciale sulla diagonale di U_F in corrispondenza della riga $|x_0, x_1\rangle$ è pari rispettivamente a $I \otimes C, C \otimes I, C \otimes C$. Questa regola è riassunta nella seguente tabella:



13 DIC. 2002



$f(x_0, x_1) = 00$	$f(x_0, x_1) = 01$	$f(x_0, x_1) = 10$	$f(x_0, x_1) = 11$
$I \otimes I$	$I \otimes C$	$C \otimes I$	$C \otimes C$

Tab. 20

In generale, nota la stringa di bit

$$f(x_0, \dots, x_{n-1}) = (z_0, \dots, z_{m-1})$$

si può immediatamente dire che il blocco matriciale sulla diagonale principale di U_F in corrispondenza della riga $|x_0, \dots, x_{n-1}\rangle$ è dato dalla seguente formula:

$$(z_0 \cdot C + (1 - z_0) \cdot I) \otimes \dots \otimes (z_{m-1} \cdot C + (1 - z_{m-1}) \cdot I)$$

Questa semplice regola è di immediata verifica e vale per tutti gli algoritmi quantistici. Essa permette di calcolare rapidamente i 2^n blocchi matriciali di U_F diversi da zero, che hanno ciascuno dimensione $2^n \times 2^n$.

Conoscendo i blocchi matriciali non nulli della matrice U_F , si può poi calcolare rapidamente il vettore A ottenuto con l'operazione di entanglement ricordando che solo un elemento per ogni riga e per ogni colonna della matrice U_F è non nullo.

Secondo una forma preferita del metodo dell'invenzione, è possibile calcolare direttamente le componenti a_k del questo vettore di entanglement A senza calcolare alcun prodotto.

Più in dettaglio, è stato osservato che, dato che gli elementi non nulli del vettore di sovrapposizione P degli algoritmi di Shor e di Simon sono dati dalla (6), solo la prima riga di ciascun blocco matriciale di dimensioni $2^n \times 2^n$ dell'operatore di entanglement U_F darebbe un contributo non nullo.

Di conseguenza, è addirittura possibile calcolare le componenti a_k del vettore di entanglement A utilizzando direttamente la seguente formula

13 DIC. 2002



$$a_k = \begin{cases} \frac{1}{2^{n/2}} & \text{se } k = f(j) + 1 + 2^n(j-1) \\ 0 & \text{altrove} \end{cases} \quad (7)$$

con $j = 1 \dots 2^n$, $k = 1 \dots 2^{2n}$.

Si ha un vettore le cui componenti o sono nulle o assumono uno stesso valore diverso da zero, che dipende solo dal numero n di qubit.

Così come per il vettore di sovrapposizione, anche in questo caso ci sono solo 2^n componenti non nulle aventi lo stesso valore, per cui il vettore di entanglement può essere determinato dagli indici delle 2^n componenti non nulle. Anche l'operazione di entanglement, così come l'operazione di sovrapposizione, può essere effettuata con un circuito che produce stringhe di bit che rappresentano questi indici e un buffer di memoria in cui memorizzare tali stringhe.

Ben più difficile è effettuare l'operazione di interferenza dell'algoritmo di Shor. Infatti, diversamente dall'operazione di entanglement, le componenti dei vettori non sono composte solo da due valori. Inoltre la presenza di prodotti tensoriali, il cui numero cresce rapidamente con n , costituisce un aspetto computazionale critico.

Per semplificare la relazione ingresso uscita, sono state considerate alcune particolari proprietà della matrice $QFT_n \otimes^n I$.

Diversamente dagli altri algoritmi quantistici, l'operazione di interferenza nell'algoritmo di Shor è eseguita mediante una trasformazione quantistica di Fourier QFT (Quantum Fourier Transformation). Così come tutti gli altri operatori quantistici, l'operatore QFT è un operatore unitario che agisce su vettori complessi dello spazio di Hilbert. Esso trasforma ciascun vettore di ingresso in una sovrapposizione di vettori di base della stessa ampiezza, ma

13 DIC. 2002



con uno spostamento di fase (phase shift).

La matrice di interferenza $QFT_n \otimes^n I$ ha solo alcuni elementi non nulli. Per la precisione, essa ha $2^n \cdot (2^n - 1)$ zeri in ciascuna colonna. Di conseguenza, non è necessario effettuare tutte le moltiplicazioni dato che molte di esse restituiscono un valore nullo.

Dette b_h le componenti del vettore B generato con l'operazione di interferenza, la parte reale e la parte immaginaria di b_h sono date dalle seguenti equazioni:

$$\begin{aligned} \text{Re}[b_h] &= \sum_{j=1}^{2^n} a_{(h \bmod 2^n) + 1 + 2^n(j-1)} \cos\left(2\pi \frac{(j-1) \cdot \text{int}[(h-1)/2^n]}{2^n}\right) \\ \text{Im}[b_h] &= \sum_{j=1}^{2^n} a_{(h \bmod 2^n) + 1 + 2^n(j-1)} \sin\left(2\pi \frac{(j-1) \cdot \text{int}[(h-1)/2^n]}{2^n}\right) \end{aligned}$$

essendo $\text{int}[\cdot]$ la funzione che restituisce la parte intera del suo argomento e con $h=1..2^{2n}$.

Ciascuna componente viene calcolata semplicemente effettuando una somma di al più 2^n funzioni coseno (o seno) e moltiplicando questa somma per $1/2^{n/2}$, perché le componenti non nulle del vettore di entanglement A sono uguali a $1/2^{n/2}$. Il vantaggio rispetto ai metodi noti è evidente, dal momento che essi prevedevano di calcolare le parti reale e immaginaria delle componenti del vettore di uscita effettuando una somma di 2^{2n} prodotti, con un costo computazionale notevolmente superiore.

13 DIC. 2002



RIVENDICAZIONI

1. Metodo di esecuzione di un algoritmo quantistico di Simon o di Shor su una data funzione ($f(x)$) codificata con un certo numero n di qubits, comprendente

eseguire un'operazione di sovrapposizione (superposition) secondo uno di detti algoritmi quantistici su un set di vettori d'ingresso, determinando un vettore di sovrapposizione (P),

eseguire un'operazione di entanglement (U_F) su detto vettore di sovrapposizione (P), determinando un corrispondente vettore di entanglement (A),

eseguire un'operazione di interferenza su detto vettore di entanglement (A) generando un corrispondente vettore di uscita (B), e

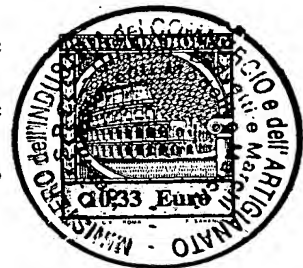
caratterizzato dal fatto che detto vettore di sovrapposizione (P) viene determinato mediante i seguenti passi di processo:

calcolare, in funzione di detto numero di qubits n , il valore ($1/2^{n/2}$) delle componenti non nulle di detto vettore di sovrapposizione (P);

calcolare indici (i) delle 2^n componenti non nulle di detto vettore di sovrapposizione come serie aritmetica di punto iniziale 1 e ragione pari a 2 elevato a detto numero n di qubits ($i = 1 + 2^n(j-1)$).

2. Il metodo della rivendicazione 1, in cui detto vettore di entanglement viene determinato mediante i seguenti passi di processo:

calcolare indici (k) delle 2^n componenti non nulle di detto vettore di entanglement (A), sommando a ciascun termine di detta successione aritmetica un relativo numero corrispondente al valore della funzione data ($f(j)$) calcolata in corrispondenza del numero di posto (j) di detto



termine in detta successione ($k = f(j) + 1 + 2^n(j-1)$);

il valore delle componenti non nulle di detto vettore di entanglement (A)

essendo uguale a quello del vettore di sovrapposizione (P).

3. Il metodo della rivendicazione 2 per eseguire un algoritmo quantistico di Shor, comprendente generare componenti reali e immaginarie ($\text{Re}[b_h]$, $\text{Im}[b_h]$) di detto vettore di uscita (B) attraverso i seguenti passi di processo:

per ogni indice h di dette componenti reali e immaginarie ($\text{Re}[b_h]$, $\text{Im}[b_h]$), verificare se tra i termini della seguente successione aritmetica

$$h \bmod 2^n + 1 + 2^n(j-1)$$

di punto iniziale $h \bmod 2^n + 1$, indice j e ragione pari a 2 elevato a detto numero n di qubits, c'è almeno un termine corrispondente ad un indice di una componente non nulla di detto vettore di entanglement;

se la verifica del punto precedente è negativa, porre dette componenti reali e immaginarie ($\text{Re}[b_h]$, $\text{Im}[b_h]$) pari a zero, altrimenti calcolare detta componente reale ($\text{Re}[b_h]$) come prodotto tra detto valore delle componenti non nulle e la somma delle seguenti funzioni coseno

$$\cos\left(2\pi \frac{(j-1) \cdot \text{int}[(h-1)/2^n]}{2^n}\right)$$

e detta componente immaginaria ($\text{Im}[b_h]$) come prodotto tra detto valore delle componenti non nulle e la somma delle seguenti funzioni seno

$$\sin\left(2\pi \frac{(j-1) \cdot \text{int}[(h-1)/2^n]}{2^n}\right)$$

per tutti i valori di detto indice j di detta successione aritmetica a cui corrispondono indici (k) di una componente non nulla di detto vettore di entanglement.



4. Gate quantistica per eseguire un algoritmo di Simon o di Shor su una data funzione ($f(x)$) codificata con un certo numero n di qubits secondo il metodo della rivendicazione 1, comprendente

un sottosistema di sovrapposizione eseguente un'operazione di sovrapposizione (superposition) secondo uno di detti algoritmi quantistici su un set di vettori d'ingresso, determinante un vettore di sovrapposizione (P),

un sottosistema di entanglement (U_F) elaborante componenti di detto vettore di sovrapposizione (P), determinante un corrispondente vettore di entanglement (A),

un sottosistema di interferenza elaborante componenti di detto vettore di entanglement (A), generando un corrispondente vettore di uscita (B),

caratterizzato dal fatto che

detto sottosistema di sovrapposizione comprende un circuito generante una prima stringa di bit rappresentativa di detto valore ($1/2^{n/2}$) delle componenti non nulle di detto vettore di sovrapposizione (P) e altre 2^n stringhe di bit ciascuna rappresentativa di un rispettivo indice (i) delle 2^n componenti non nulle di detto vettore di sovrapposizione;

un buffer di memoria memorizzante le stringhe rappresentanti detto valore ($1/2^{n/2}$) e detti indici (i).

5. La gate quantistica della rivendicazione 4 implementante il metodo della rivendicazione 2, in cui detto sistema di entanglement comprende

un circuito generante stringhe di bit rappresentative di detti indici (k) delle 2^n componenti non nulle di detto vettore di entanglement (A);

1 3 DIC. 2002



un secondo buffer di memoria memorizzante dette stringhe di bit (k).

p.p. STMicroelectronics S.r.l.

Il Mandatario Gaetano Barbaro

Gaetano BARBARO
N° Iscr. Albo 994 B

(Società Italiana Brevetti S.p.A.)

BI346V



(Luca De Zorzi)

13 DIC. 2002

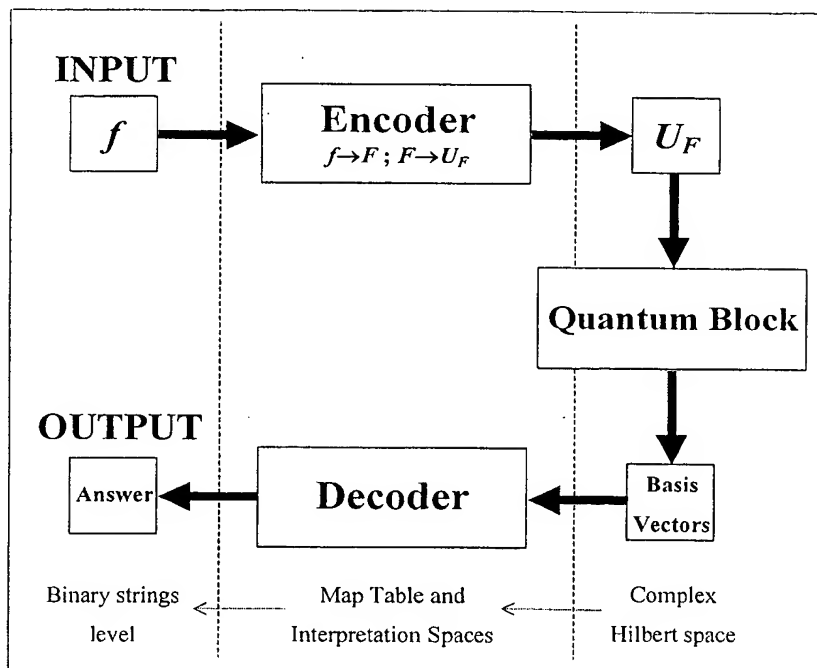


FIG. 1

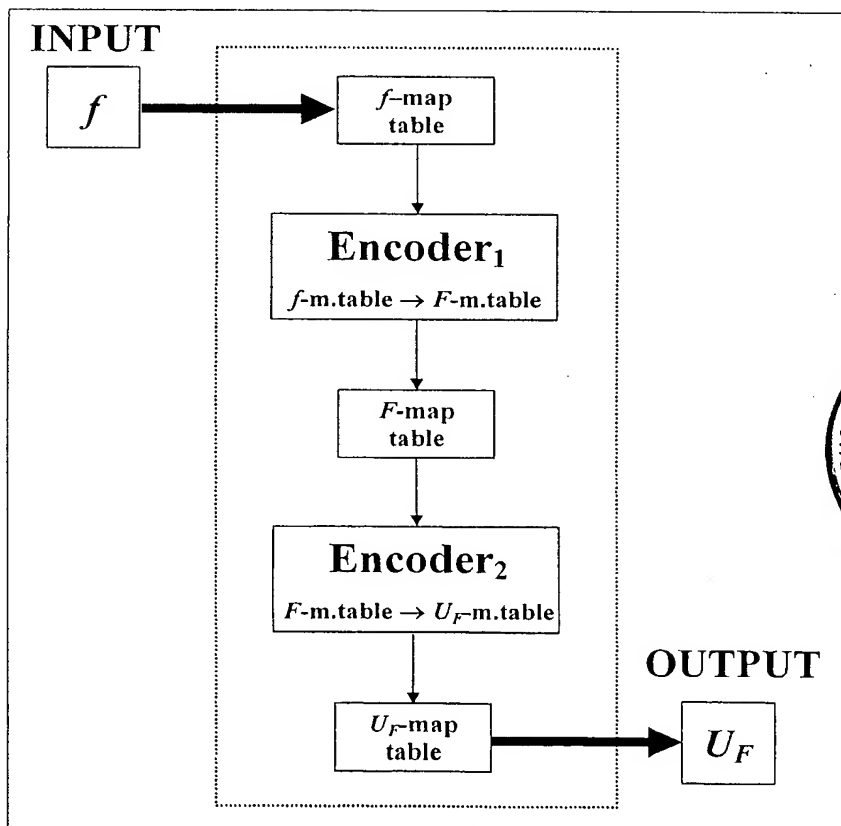
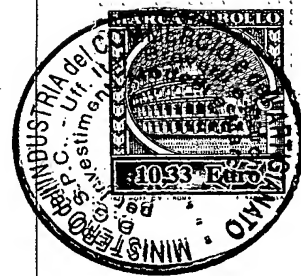


FIG. 2



Gaetano BARBARO
N° Iscr. Albo 994 B

[Handwritten signature]
13 Dic 2002

13 DIC. 2002

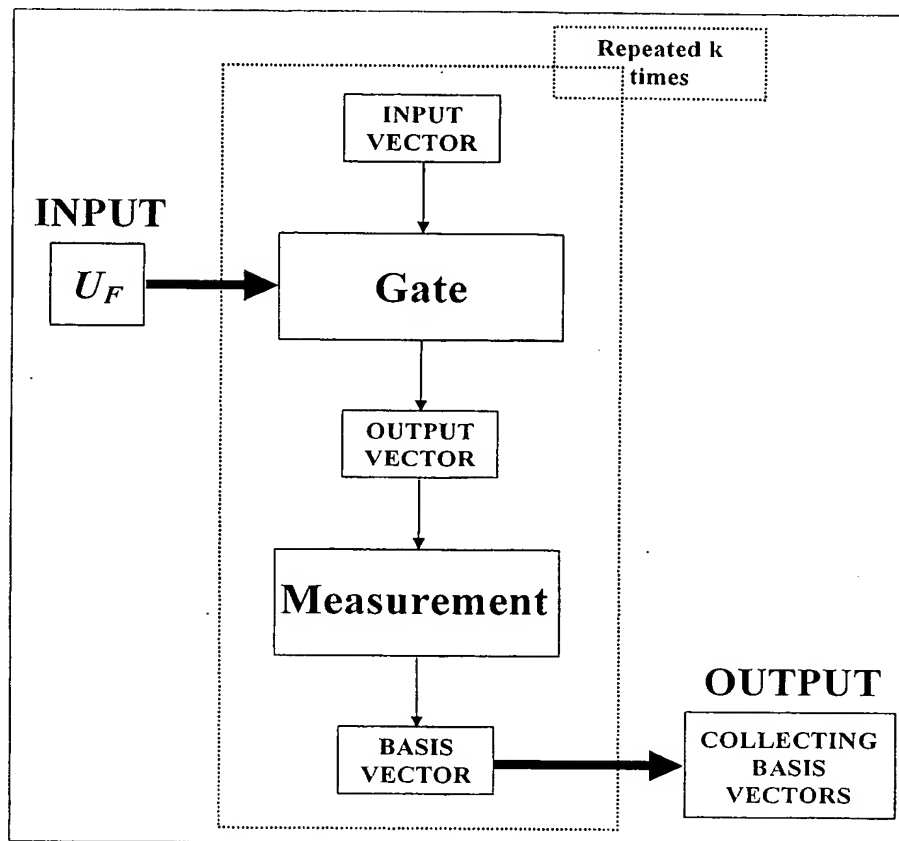


FIG. 3

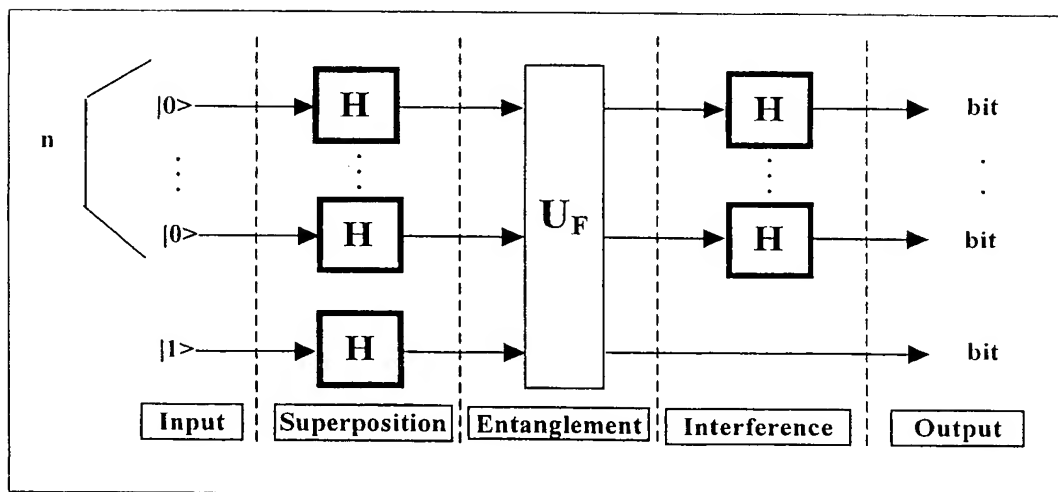


FIG. 4



Handwritten signature of Gaetano Barbaro

Gaetano BARBARO
N° Iscr. Albo 994 B

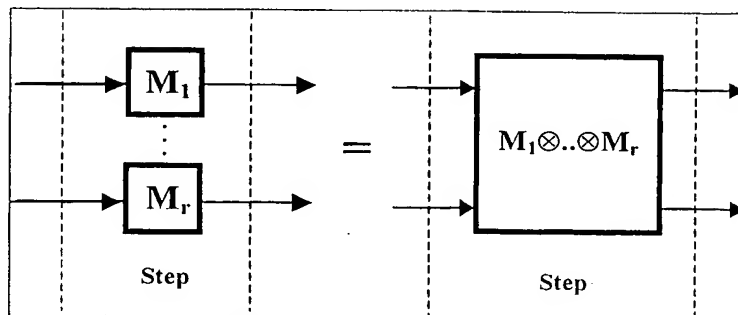


FIG. 5A

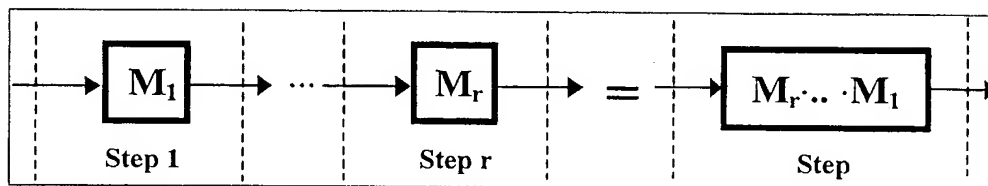


FIG. 5B

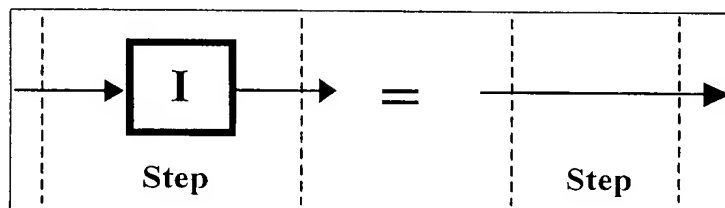


FIG. 5C

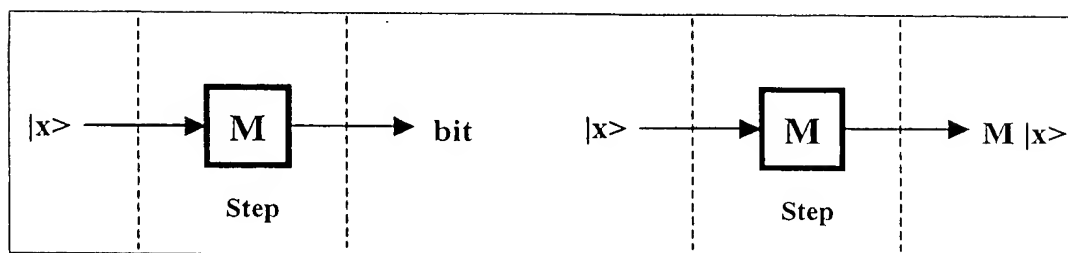


FIG. 5D

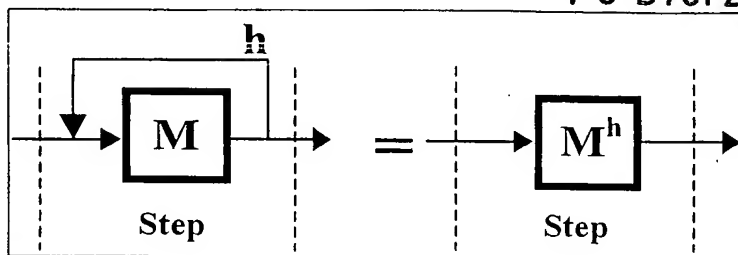


FIG. 5E

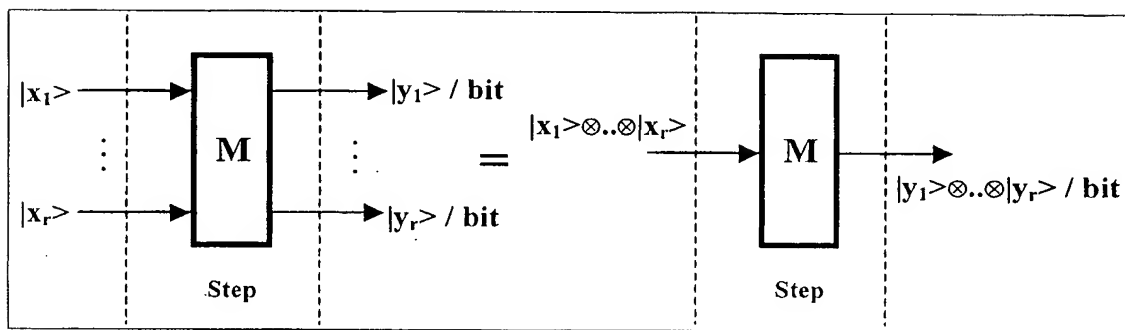


FIG. 5F

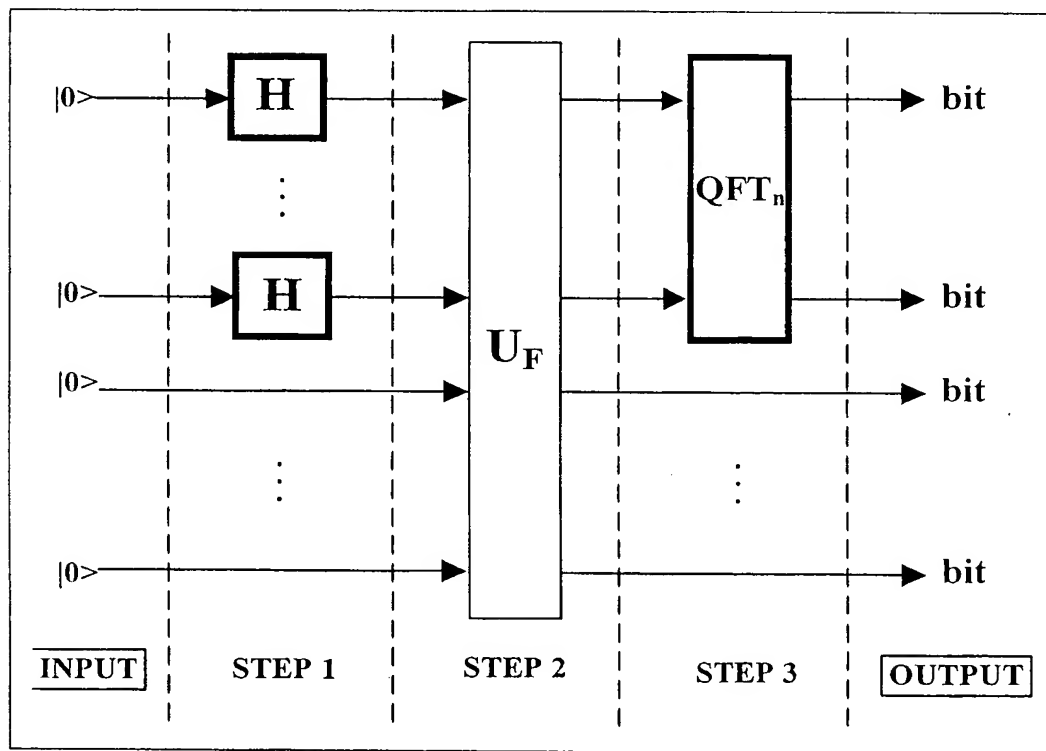


FIG. 6

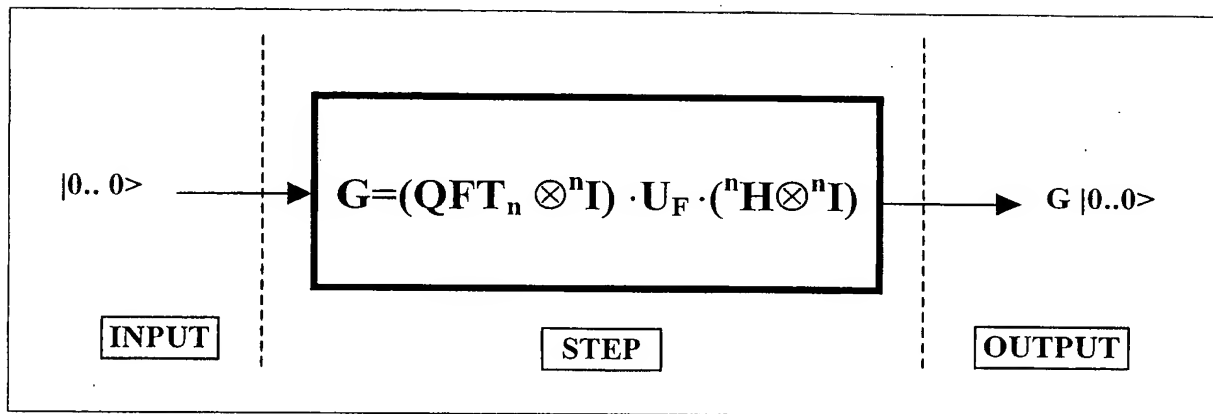


FIG. 7

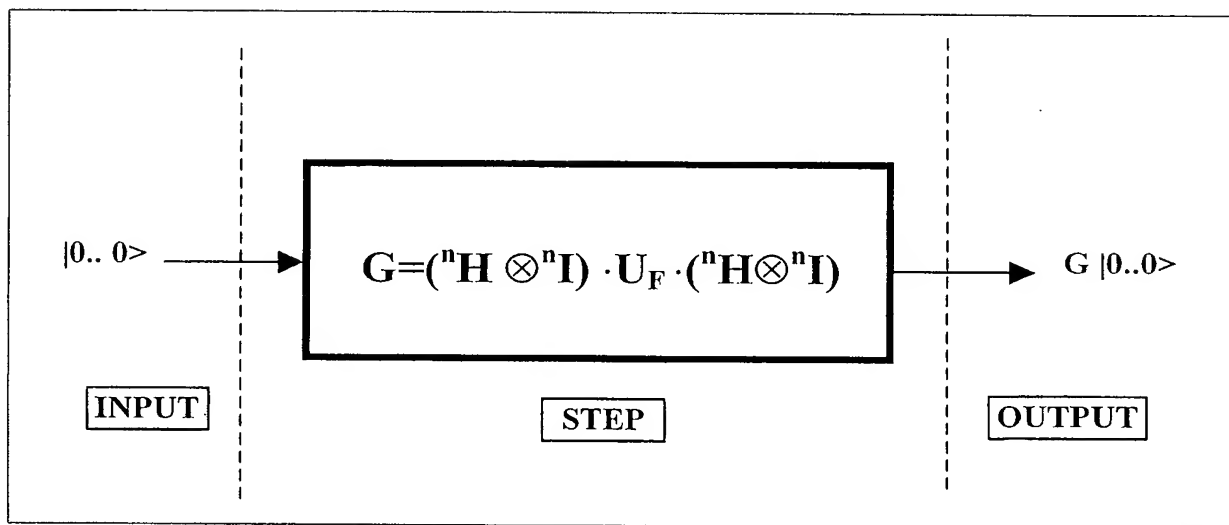


FIG. 8



Luca De Zorzi

Gaetano BARBARO
N° Iscr. Albo 994 B